



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/667,804	09/22/2003	Linwood Hugh Overby JR.	5577-284	2160
7590 02/20/2007 David K. Purks Myers Bigel Sibley & Sajovec, P.A. P.O. Box 37428 Raleigh, NC 27627			EXAMINER TO, BAOTRAN N	
			ART UNIT 2135	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
3 MONTHS			02/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	Application No. 10/667,804	Applicant(s) OVERBY, LINWOOD HUGH	
	Examiner Bao Tran N. To	Art Unit 2135	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 22 September 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 September 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>20030922</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1-31 are pending in the application.

#### ***Information Disclosure Statement***

2. The information disclosure statement (IDS) submitted on 09/22/2003. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

#### ***Drawings***

3. The drawings are objected to because the conditional label between element 520 and 530 in figure 5 is "NO", it should be labeled "YES". Appropriate correction is required. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an

application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Aucsmith et al. (U.S. Patent Application Publication 2003/0110392 A1) hereinafter Aucsmith.

Regarding Claims 1 and 26, Aucsmith discloses a method of responding to an intrusion, the method comprising:

selectively responding to at least one notification of an intrusion (paragraph 0055), from a network-accessible intrusion detection service manager (Figure 1) (paragraph 0027), by a computer (Figure 1, element 104) evaluating the notification

based on local IDS policy that includes information relating to the notification of an intrusion and information related to the computer (paragraph 0055).

Regarding Claim 15, Aucsmith discloses a computer system that responds to intrusions, the computer system comprising:

a plurality of computers (Figure 1, elements 102(1 to N)), each comprising a local IDS policy (paragraphs 0027, 0038 and 0070);

an intrusion detection service (IDS) manager (element 104/106) that is configured to generate for the computers at least one notification of an intrusion (Figure 1, paragraph 0055), and wherein each of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to the computer (paragraph 0051-0055).

Regarding Claim 2, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on whether the computer is a firewall for other computers in the computer system (Figure 1, element 112).

Regarding Claims 3, 21 and 29, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on whether the computer is a server of information for other computers in the computer system (Figure 1, paragraphs 0030, 0033 and 0051-0055).

Regarding Claim 4, Aucsmith discloses the limitations of Claim 3 above. Aucsmith further discloses evaluating whether the computer serves as at least one of a webserver, an intranet application server, and a backend server (paragraphs 0025 and 0027).

Regarding Claims 5, 22, and 30, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on whether the computer is protected by a firewall from a source of the intrusion (Figure 1, element 112, paragraphs 0030, 0033 and 0051-0055).

Regarding Claim 6, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on memory utilization in the computer (paragraph 0084).

Regarding Claim 7, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on processor utilization in the computer (paragraph 0084).

Regarding Claim 8, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on

information from other than the IDS manager that indicates an intrusion into the computer (Figure 1, elements 116 and 120, paragraph 0026 –0028).

Regarding Claims 9 and 25, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on proximity of the computer to a source of the intrusion (paragraphs 0028 and 0051-0055).

Regarding Claims 10, 20 and 27, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses downloading the local IDS policy from a network-accessible repository to the computer (paragraphs 0028, 0078 and 0083).

Regarding Claims 11 and 28, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the local IDS policy comprises one or more response actions to be taken based on a notification from the network-accessible IDS manager of an intrusion (paragraph 0050).

Regarding Claim 12, Aucsmith discloses the limitations of Claim 11 above. Aucsmith further discloses wherein the response action comprises terminating an application that is a target of an attack (paragraph 0037).

Regarding Claim 13, Aucsmith discloses the limitations of Claim 11 above. Aucsmith further discloses wherein the response action comprises discarding information in a communication to the computer (paragraph 0037).

Regarding Claim 14, Aucsmith discloses the limitations of Claim 11 above. Aucsmith further discloses wherein the response action comprises discontinuing communication with a source of the communication (paragraph 0039).

Regarding Claim 16, Aucsmith discloses the limitations of Claim 15 above. Aucsmith further discloses wherein the IDS manager is configured to determine that an intrusion has occurred in the computer system, and is configured to generate a notification based on determining that an intrusion has occurred (paragraph 0045).

Regarding Claim 17, Aucsmith discloses the limitations of Claim 16 above. Aucsmith further discloses wherein at least two of the computers respond differently to the same intrusion notification from the IDS manager (paragraph 0055).

Regarding Claim 18, Aucsmith discloses the limitations of Claim 16 above. Aucsmith further discloses wherein at least one of the computers responds differently to the same intrusion notification repeated at least once over time (paragraph 0055).

Regarding Claim 19, Aucsmith discloses the limitations of Claim 15 above. Aucsmith further discloses a plurality of sensors that are configured to sense events that may indicate one or more possible intrusions into the computer system, and that are configured to inform the IDS manager of the events, and wherein the IDS manager is configured to determine that an intrusion has occurred in the computer system by correlating the events from the sensors (Figures 1 and 2, elements 106(1-N) and step 210, paragraphs 0035 and 0041).

Regarding Claims 23 and 31, Aucsmith discloses the limitations of Claim 15 above. Aucsmith further discloses wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy and based on at least one of memory utilization in the computer and processor utilization in the computer (paragraph 0084).

Regarding Claim 24, Aucsmith discloses the limitations of Claim 15 above. Aucsmith further discloses wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to possible intrusions into the computer (paragraphs 0051-0055).

#### ***Prior Art***

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

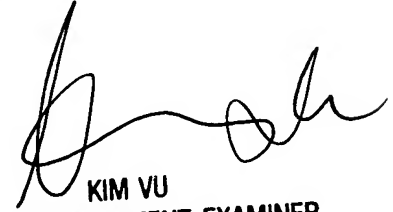
***Contact Information***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BT  
02/06/2007

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100